RSAC | 2025 Conference

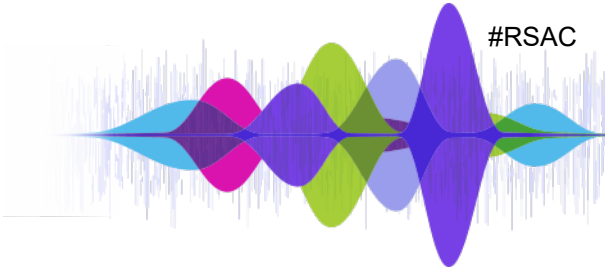
Many Voices.
One Community.

SESSION ID: FND-M05

Building a Resilient Cloud Security Foundation

Rich Mogull

SVP Cloud Security | | CEO
FireMon | | Securosis
www.linkedin.com/in/richmogull



Disclaimer

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference LLC does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

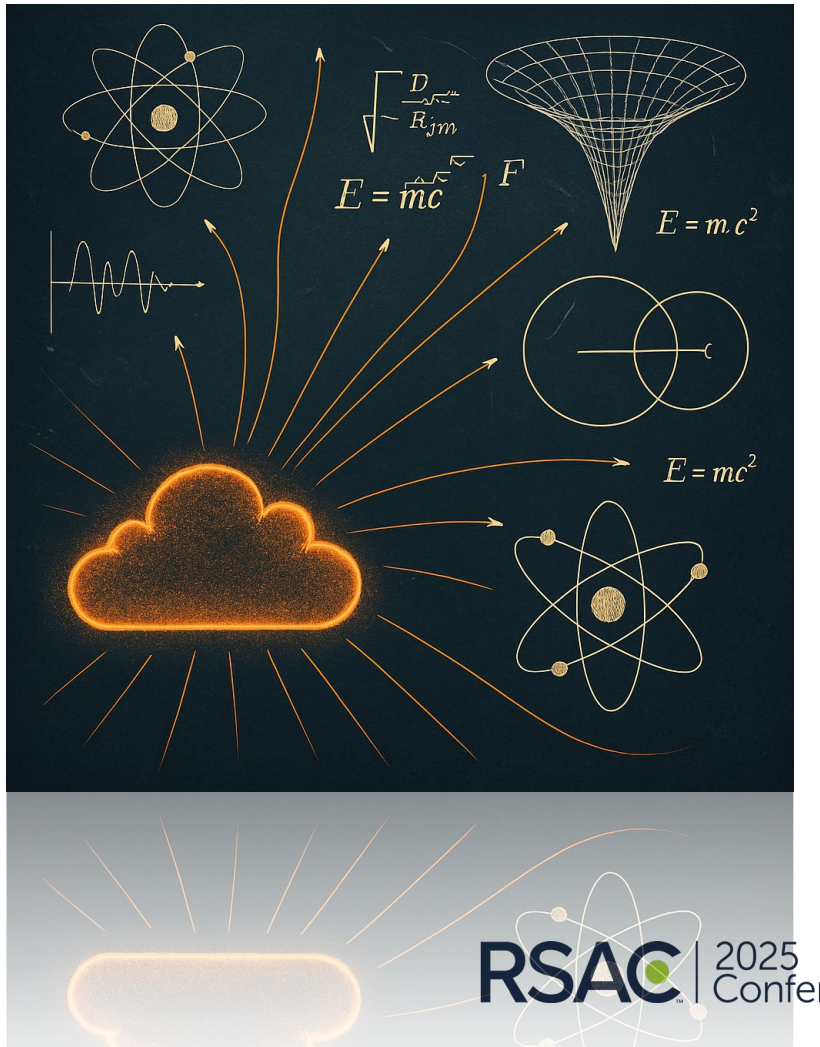
Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

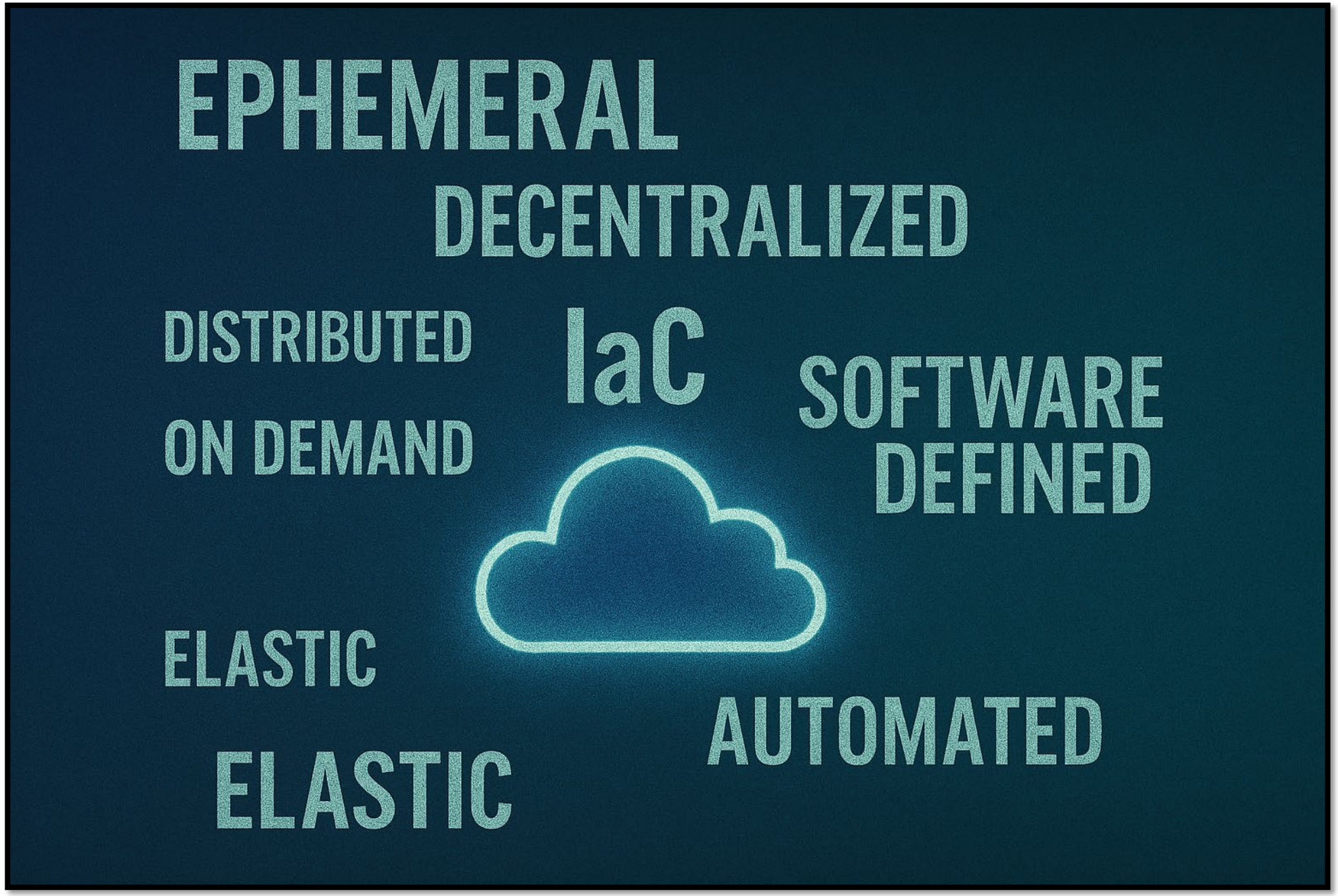
© 2025 RSA Conference LLC or its affiliates. The RSAC and RSAC CONFERENCE logos and other trademarks are proprietary. All rights reserved.

How (and Why) Cloud Changes Everything

- Cloud is decentralized
  - Enterprise security and governance were designed for centralization and scarcity
- But cloud administration is unified
  - Single consoles/portals/APIs
- All protected with little more than a username and password

The Grand Unified Theory of Cloud Governance




EPHEMERAL
DECENTRALIZED
DISTRIBUTED
IaC
SOFTWARE DEFINED
ON DEMAND
ELASTIC
AUTOMATED
ELASTIC

Cloud Security Needs Cloud Specific Guidance

- There are nearly no effective cloud-native security frameworks
  - NIST CSF and 800-53 have not been effectively updated for cloud computing
  - There are gaps in every framework because they try to align with previous frameworks
  - Cloud is fast, automated, and decentralized; “security standards” in the traditional sense can’t keep up

“Let the past die. kill it if you have to. That's the only way you can become what you were meant to be.”

Cloud Security Maturity Model

Version 2.0

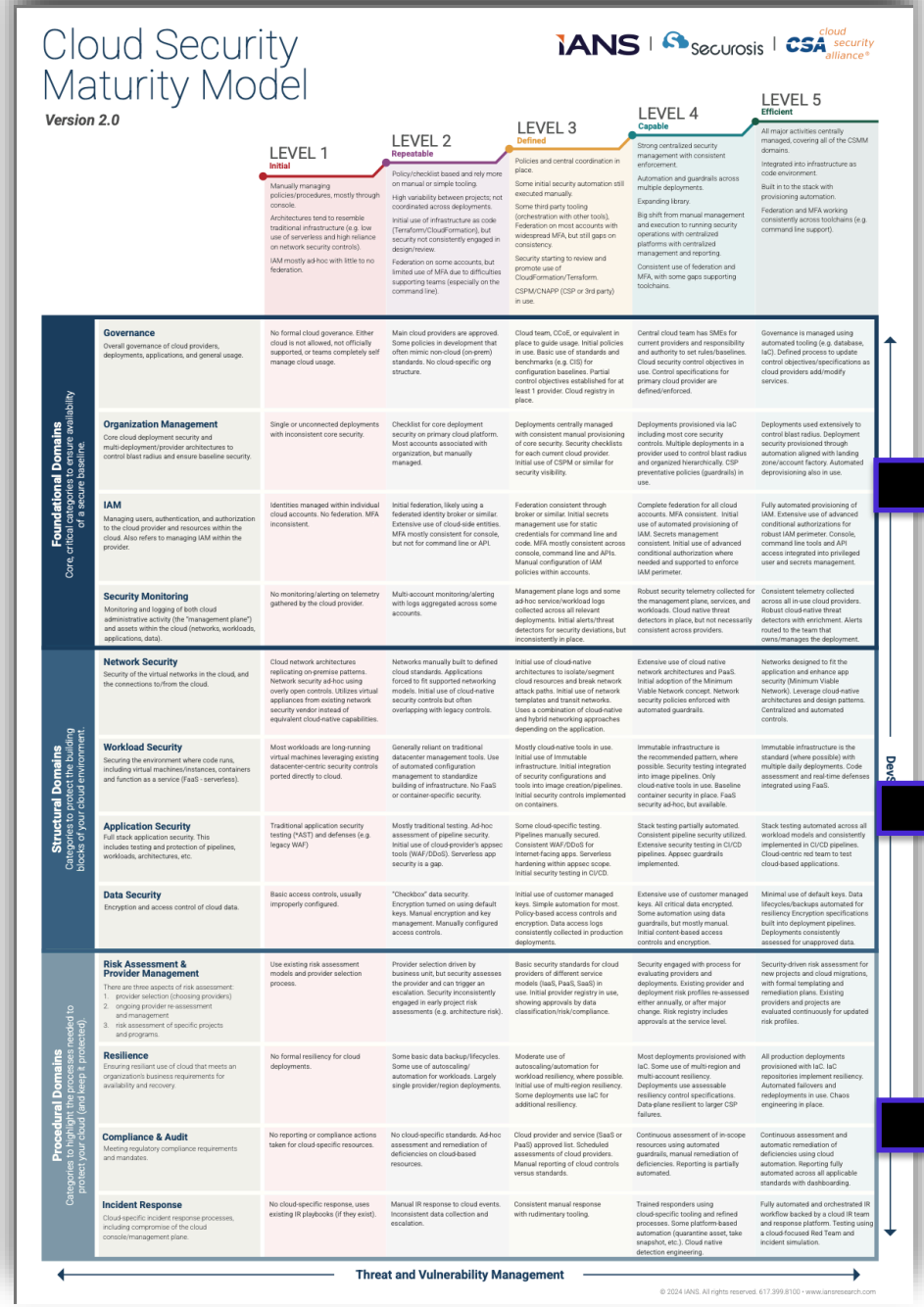
IANS | Securosis | CSA cloud security alliance®

	LEVEL 1 Initial	LEVEL 2 Repeatable	LEVEL 3 Defined	LEVEL 4 Capable	LEVEL 5 Efficient
	Manually managing policies/procedures, mostly through console. Architectures tend to resemble traditional infrastructure (e.g. low use of serverless and high reliance on network security controls). IAM mostly ad-hoc with little to no federation.	Policy/checklist based and rely more on manual or simple tooling. High variability between projects; not coordinated across deployments. Initial use of infrastructure as code (Terraform/CloudFormation), but security not consistently engaged in design/review. Federation on some accounts, but limited use of MFA due to difficulties supporting teams (especially on the command line).	Policies and central coordination in place. Some initial security automation still executed manually. Some third party tooling (orchestration with other tools). Federation on most accounts with widespread MFA, but still gaps on consistency. Security starting to review and promote use of CloudFormation/Terraform. CSPM/CNAPP (CSP or 3rd party) in use.	Strong centralized security management with consistent enforcement. Automation and guardrails across multiple deployments. Expanding library. Big shift from manual management and execution to running security operations with centralized platforms with centralized management and reporting. Consistent use of federation and MFA, with some gaps supporting toolchains.	All major activities centrally managed, covering all of the CSMM domains. Integrated into infrastructure as code environment. Built in to the stack with provisioning automation. Federation and MFA working consistently across toolchains (e.g. command line support).
Foundational Domains Core, critical categories to ensure availability of a secure baseline.					
Governance Overall governance of cloud providers, deployments, applications, and general usage.	No formal cloud governance. Either cloud is not allowed, not officially supported, or teams completely self manage cloud usage.	Main cloud providers are approved. Some policies in development that often mimic non-cloud (on-prem) standards. No cloud-specific org structure.	Cloud team, CCoE, or equivalent in place to guide usage. Initial policies in use. Basic use of standards and benchmarks (e.g. CIS) for configuration baselines. Partial control objectives established for at least 1 provider. Cloud registry in place.	Central cloud team has SMEs for current providers and responsibility and authority to set rules/baselines. Cloud security control objectives in use. Control specifications for primary cloud provider are defined/enforced.	Governance is managed using automated tooling (e.g. database, IaC). Defined process to update control objectives/specifications as cloud providers add/modify services.
Organization Management Core cloud deployment security and multi-deployment/provider architectures to control blast radius and ensure baseline security.	Single or unconnected deployments with inconsistent core security.	Checklist for core deployment security on primary cloud platform. Most accounts associated with organization, but manually managed.	Deployments centrally managed with consistent manual provisioning of core security. Security checklists for each current cloud provider. Initial use of CSPM or similar for security visibility.	Deployments provisioned via IaC including most core security controls. Multiple deployments in a provider used to control blast radius and organized hierarchically. CSP preventative policies (guardrails) in use.	Deployments used extensively to control blast radius. Deployment security provisioned through automation aligned with landing zone/account factory. Automated deprovisioning also in use.
IAM Managing users, authentication, and authorization to the cloud provider and resources within the cloud. Also refers to managing IAM within the provider.	Identities managed within individual cloud accounts. No federation. MFA inconsistent.	Initial federation, likely using a federated identity broker or similar. Extensive use of cloud-side entities. MFA mostly consistent for console, but not for command line or API.	Federation consistent through broker or similar. Initial secrets management use for static credentials for command line and code. MFA mostly consistent across console, command line and APIs. Manual configuration of IAM policies within accounts.	Complete federation for all cloud accounts. MFA consistent. Initial use of automated provisioning of IAM. Secrets management consistent. Initial use of advanced conditional authorization where needed and supported to enforce IAM perimeter.	Fully automated provisioning of IAM. Extensive use of advanced conditional authorizations for robust IAM perimeter. Console, command line tools and API access integrated into privileged user and secrets management.
Security Monitoring Monitoring and logging of both cloud administrative activity (the "management plane") and assets within the cloud (networks, workloads, applications, data).	No monitoring/alerting on telemetry gathered by the cloud provider.	Multi-account monitoring/alerting with logs aggregated across some accounts.	Management plane logs and some ad-hoc service/workload logs collected across all relevant deployments. Initial alerts/threat detectors for security deviations, but inconsistently in place.	Robust security telemetry collected for the management plane, services, and workloads. Cloud native threat detectors in place, but not necessarily consistent across providers.	Consistent telemetry collected across all in-use cloud providers. Robust cloud-native threat detectors with enrichment. Alerts routed to the team that owns/manages the deployment.
Structural Domains Categories to protect the building blocks of your cloud environment.					
Network Security Security of the virtual networks in the cloud, and the connections to/from the cloud.	Cloud network architectures replicating on-premise patterns. Network security ad-hoc using overly open controls. Utilizes virtual appliances from existing network security vendor instead of equivalent cloud-native capabilities.	Networks manually built to defined cloud standards. Applications forced to fit supported networking models. Initial use of cloud-native security controls but often overlapping with legacy controls.	Initial use of cloud-native architectures to isolate/segment cloud resources and break network attack paths. Initial use of network templates and transit networks. Uses a combination of cloud-native and hybrid networking approaches depending on the application.	Extensive use of cloud native network architectures and PaaS. Initial adoption of the Minimum Viable Network concept. Network security policies enforced with automated guardrails.	Networks designed to fit the application and enhance app security (Minimum Viable Network). Leverage cloud-native architectures and design patterns. Centralized and automated controls.
Workload Security Securing the environment where code runs, including virtual machines/instances, containers and function as a service (FaaS - serverless).	Most workloads are long-running virtual machines leveraging existing datacenter-centric security controls ported directly to cloud.	Generally reliant on traditional datacenter management tools. Use of automated configuration management to standardize building of infrastructure. No FaaS or container-specific security.	Mostly cloud-native tools in use. Initial use of immutable infrastructure. Initial integration of security configurations and tools into image creation/pipelines. Initial security controls implemented on containers.	Immutable infrastructure is the recommended pattern, where possible. Security testing integrated into image pipelines. Only cloud-native tools in use. Baseline container security in place. FaaS security ad-hoc, but available.	Immutable infrastructure is the standard (where possible) with multiple daily deployments. Code assessment and real-time defenses integrated using FaaS.
Application Security Full stack application security. This includes testing and protection of pipelines, workloads, architectures, etc.	Traditional application security testing (*AST) and defenses (e.g. legacy WAF)	Mostly traditional testing. Ad-hoc assessment of pipeline security. Initial use of cloud-provider's appsec tools (WAF/DDoS). Serverless app security is a gap.	Some cloud-specific testing. Pipelines manually secured. Consistent WAF/DDoS for Internet-facing apps. Serverless hardening within appsec scope. Initial security testing in CI/CD.	Stack testing partially automated. Consistent pipeline security utilized. Extensive security testing in CI/CD pipelines. Appsec guardrails implemented.	Stack testing automated across all workload models and consistently implemented in CI/CD pipelines. Cloud-centric red team to test cloud-based applications.
Data Security Encryption and access control of cloud data.	Basic access controls, usually improperly configured.	"Checkbox" data security. Encryption turned on using default keys. Manual encryption and key management. Manually configured access controls.	Initial use of customer managed keys. Simple automation for most. Policy-based access controls and encryption. Data access logs consistently collected in production deployments.	Extensive use of customer managed keys. All critical data encrypted. Some automation using data guardrails, but mostly manual. Initial content-based access controls and encryption.	Minimal use of default keys. Data lifecycles/backups automated for resiliency. Encryption specifications built into deployment pipelines. Deployments consistently assessed for unapproved data.
Procedural Domains Categories to highlight the processes needed to protect your cloud (and keep it protected).					
Risk Assessment & Provider Management There are three aspects of risk assessment: 1. provider selection (choosing providers) 2. ongoing provider re-assessment and management 3. risk assessment of specific projects and programs.	Use existing risk assessment models and provider selection process.	Provider selection driven by business unit, but security assesses the provider and can trigger an escalation. Security inconsistently engaged in early project risk assessments (e.g. architecture risk).	Basic security standards for cloud providers of different service models (IaaS, PaaS, SaaS) in use. Initial provider registry in use, showing approvals by data classification/risk/compliance.	Security engaged with process for evaluating providers and deployments. Existing provider and deployment risk profiles re-assessed either annually, or after major change. Risk registry includes approvals at the service level.	Security-driven risk assessment for new projects and cloud migrations, with formal templating and remediation plans. Existing providers and projects are evaluated continuously for updated risk profiles.
Resilience Ensuring resilient use of cloud that meets an organization's business requirements for availability and recovery.	No formal resiliency for cloud deployments.	Some basic data backup/lifecycles. Some use of autoscaling/ automation for workloads. Largely single provider/region deployments.	Moderate use of autoscaling/automation for workload resiliency, where possible. Initial use of multi-region resiliency. Some deployments use IaC for additional resiliency.	Most deployments provisioned with IaC. Some use of multi-region and multi-account resiliency. Deployments use assessable resiliency control specifications. Data-plane resilient to larger CSP failures.	All production deployments provisioned with IaC. IaC repositories implement resiliency. Automated failovers and redeployments in use. Chaos engineering in place.
Compliance & Audit Meeting regulatory compliance requirements and mandates.	No reporting or compliance actions taken for cloud-specific resources.	No cloud-specific standards. Ad-hoc assessment and remediation of deficiencies on cloud-based resources.	Cloud provider and service (SaaS or PaaS) approved list. Scheduled assessments of cloud providers. Manual reporting of cloud controls versus standards.	Continuous assessment of in-scope resources using automated guardrails, manual remediation of deficiencies. Reporting is partially automated.	Continuous assessment and automatic remediation of deficiencies using cloud automation. Reporting fully automated across all applicable standards with dashboarding.
Incident Response Cloud-specific incident response processes, including compromise of the cloud console/management plane.	No cloud-specific response, uses existing IR playbooks (if they exist).	Manual IR response to cloud events. Inconsistent data collection and escalation.	Consistent manual response with rudimentary tooling.	Trained responders using cloud-specific tooling and refined processes. Some platform-based automation (quarantine asset, take snapshot, etc.). Cloud native detection engineering.	Fully automated and orchestrated IR workflow backed by a cloud IR team and response platform. Testing using a cloud-focused Red Team and incident simulation.

DevSecOps

Threat and Vulnerability Management

© 2024 IANS. All rights reserved. 617.399.8100 • www.iansresearch.com



Where to start

Core shared security services for good governance

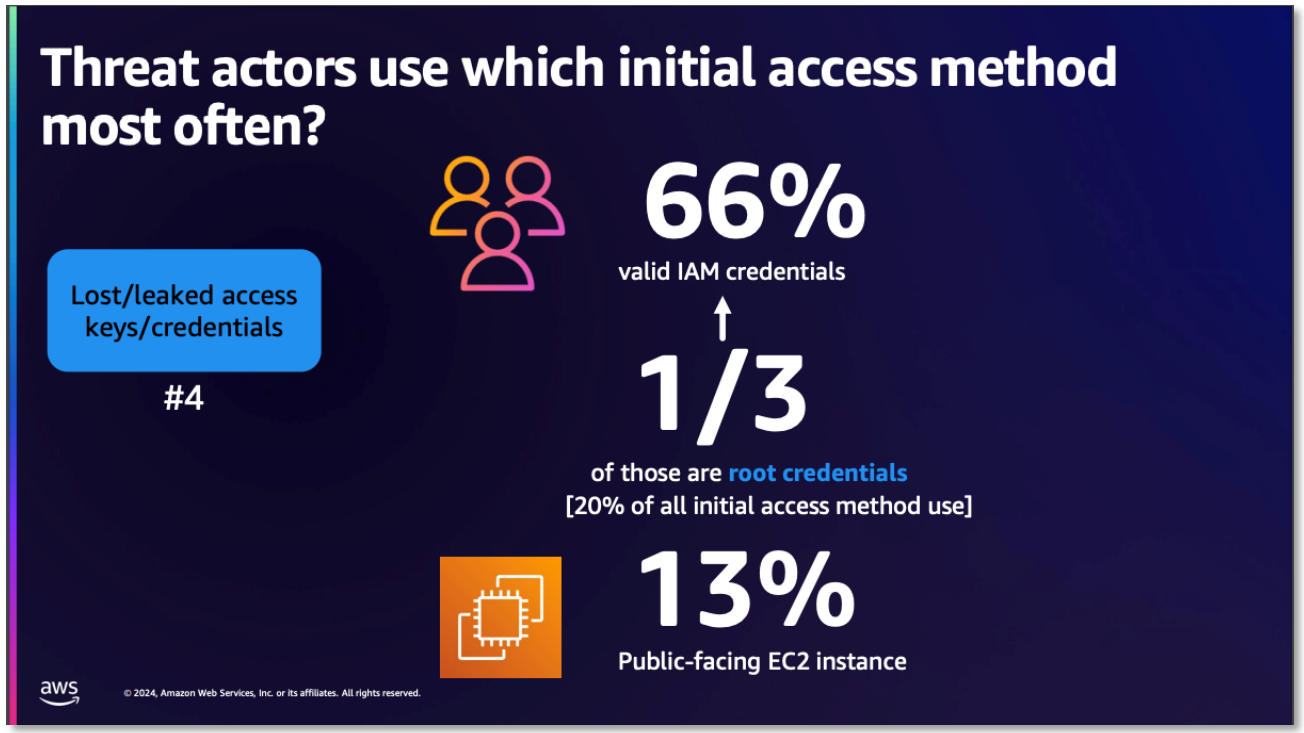
Build together

App/deployment-specific security that will change for different scenarios

Mature together

Essential long-term processes to stay secure and compliant

Align to actual threats



- Nearly all cloud security incidents are two things:
  - Exposed/lost/stolen credentials
  - Public facing thing that gets hacked
- (You can ignore most everything else)

K.I.S.S.

K.I.S.S.

1-2 Takeaways per category

RSAC | 2025 Conference

The Foundation

Core Shared Services for a Resilient Organization

Many Voices.
One Community.

All cloud security failures are governance failures

Put someone in charge

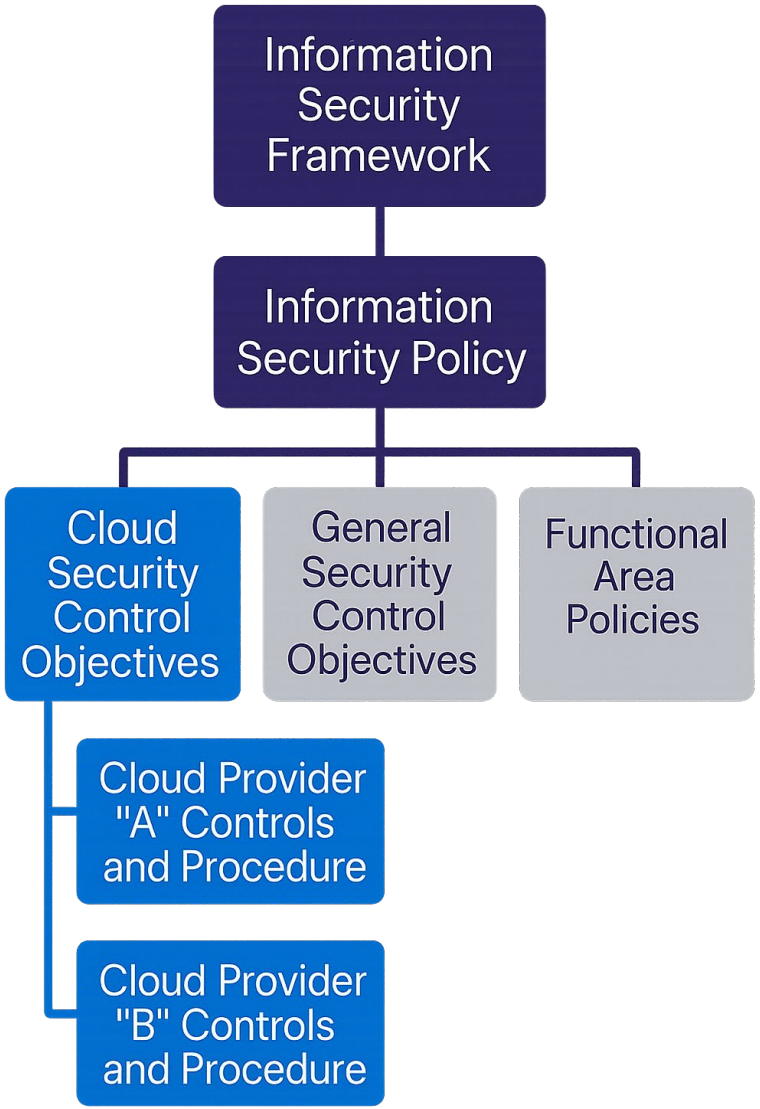
Train them on cloud

Get executive support

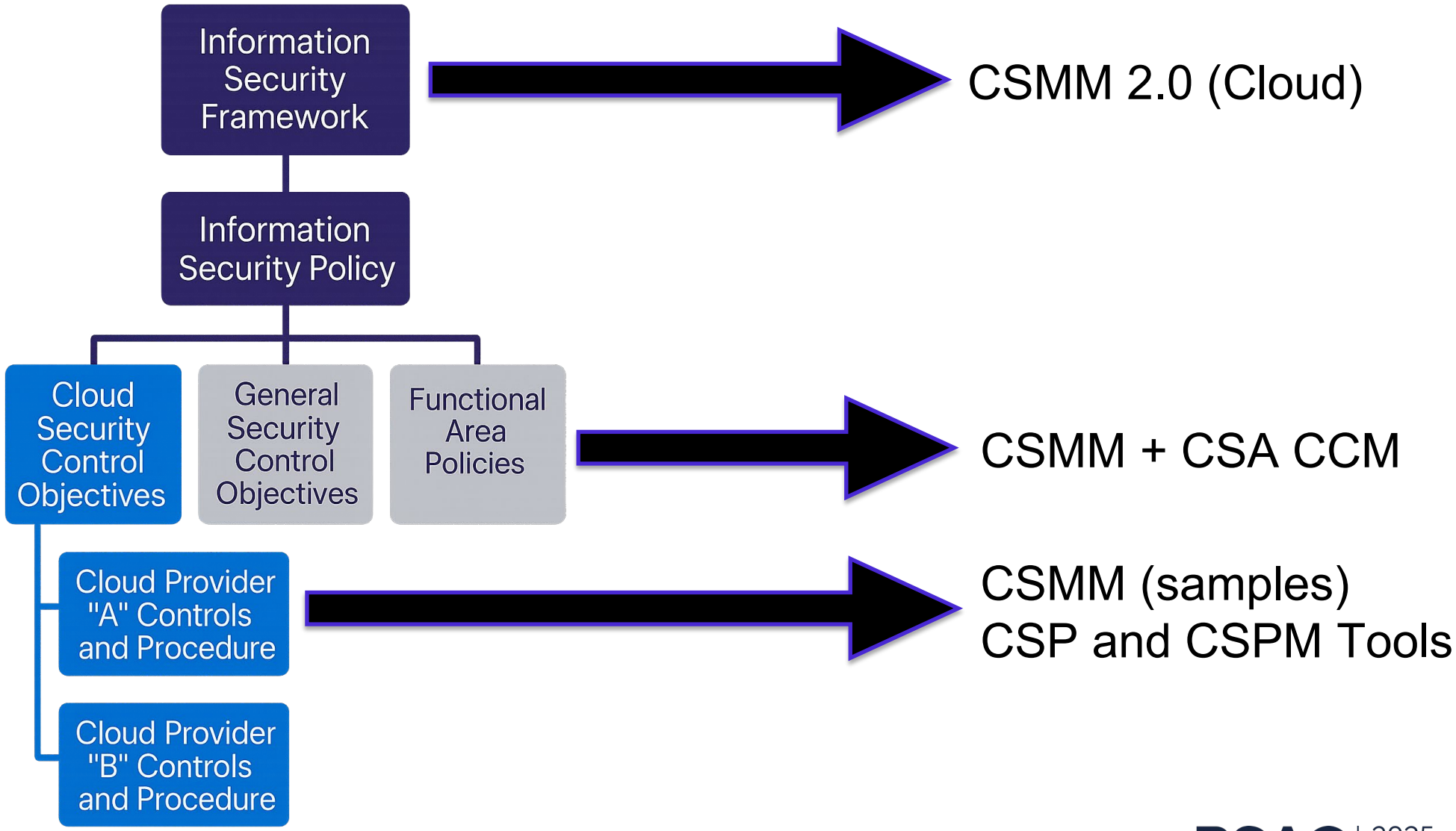
Treat cloud as cloud

Lack of clear lines of authority, security “blocked out”, security “is a blocker”, and failure to build cloud-specific knowledge and processes always lead to failure

The Governance Hierarchy


Information Security Framework
Information Security Policy
Cloud Security Control Objectives
General Security Control Objectives
Functional Area Policies
Cloud Provider "A" Controls and Procedure
Cloud Provider "B" Controls and Procedure

The Governance Hierarchy



The Base: Core Policy Types All Providers Support

Organization-Based Policies

What is allowed within a deployment (the security blanket)

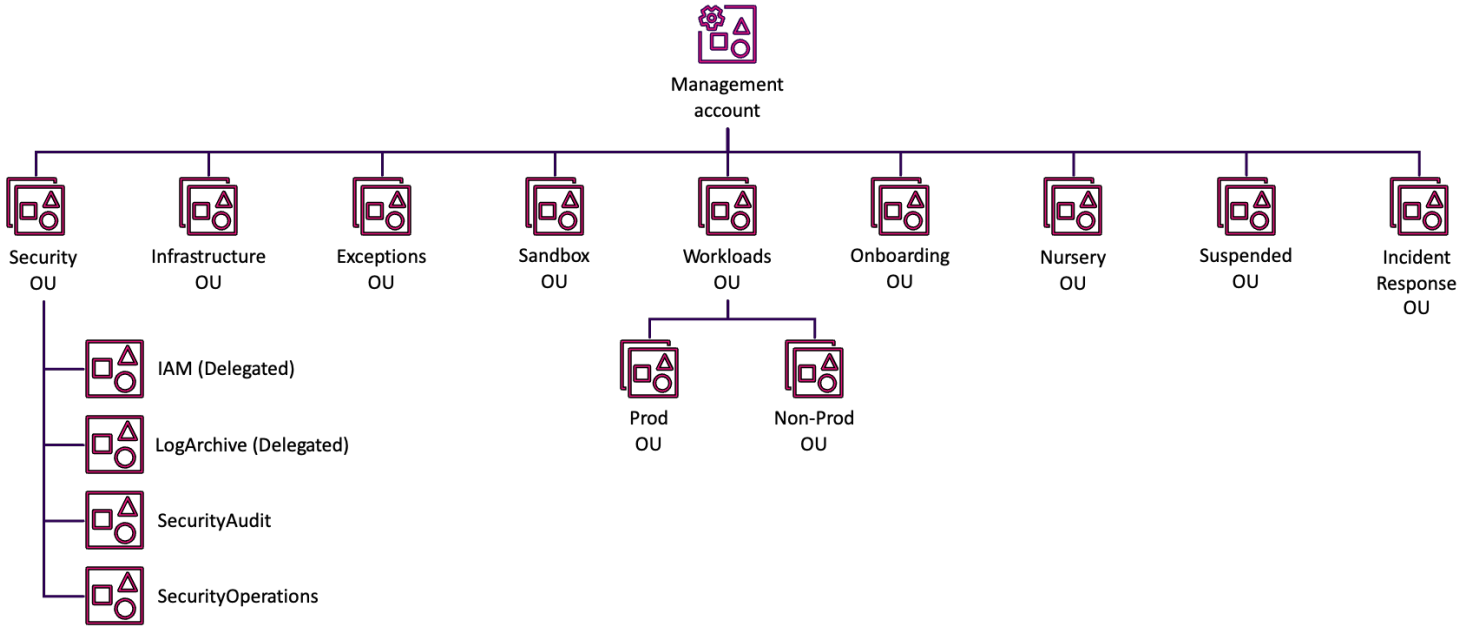
Identity-Based Policies

What an identity is allowed to do

Resource-Based Policies

How a resource can be accessed and used

Organization Management



Required for effective:

- CSPM
- Organization policies
- SSO/IAM
  - Identity-based policies
- Shared Services

IAM

No Static Credentials

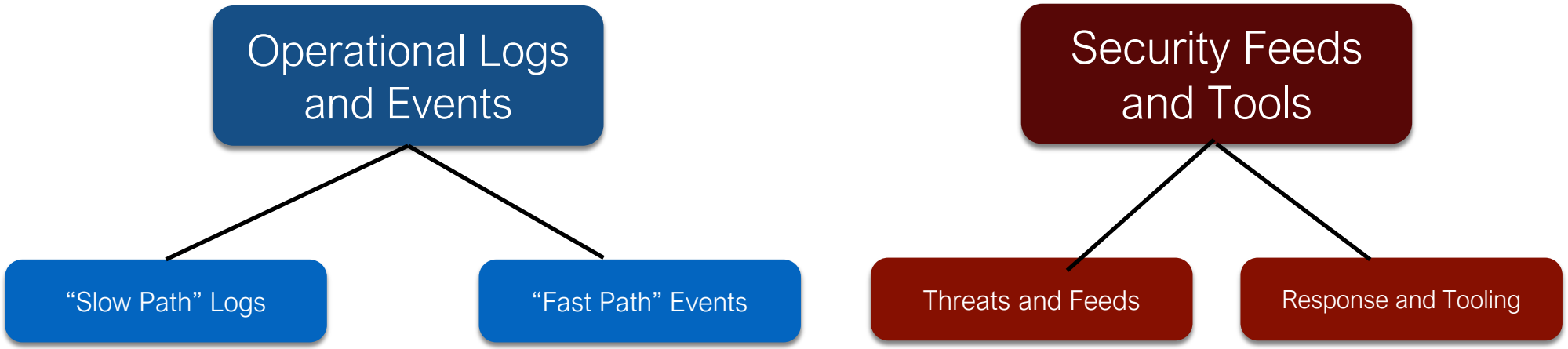
SSO+MFA for Humans

JIT for Admins

Infosec Reviews

Scan IaC and Live

Security Telemetry



- Feeds and speeds
  - Events
  - Logs
  - Tool-based events

Misconfigs as Vulns and Incidents

CSPM/CNAPP
Finding

?

Mistake

Violation

Vulnerability

Attack

Apply: Foundational

- Establish clear governance, in person and on paper
- Get rid of static credentials for humans
  - Use JIT for admins
- Use organization-based policies
- Deploy a CSPM
- You know how to handle logs, now learn about cloud native events

RSAC | 2025 Conference

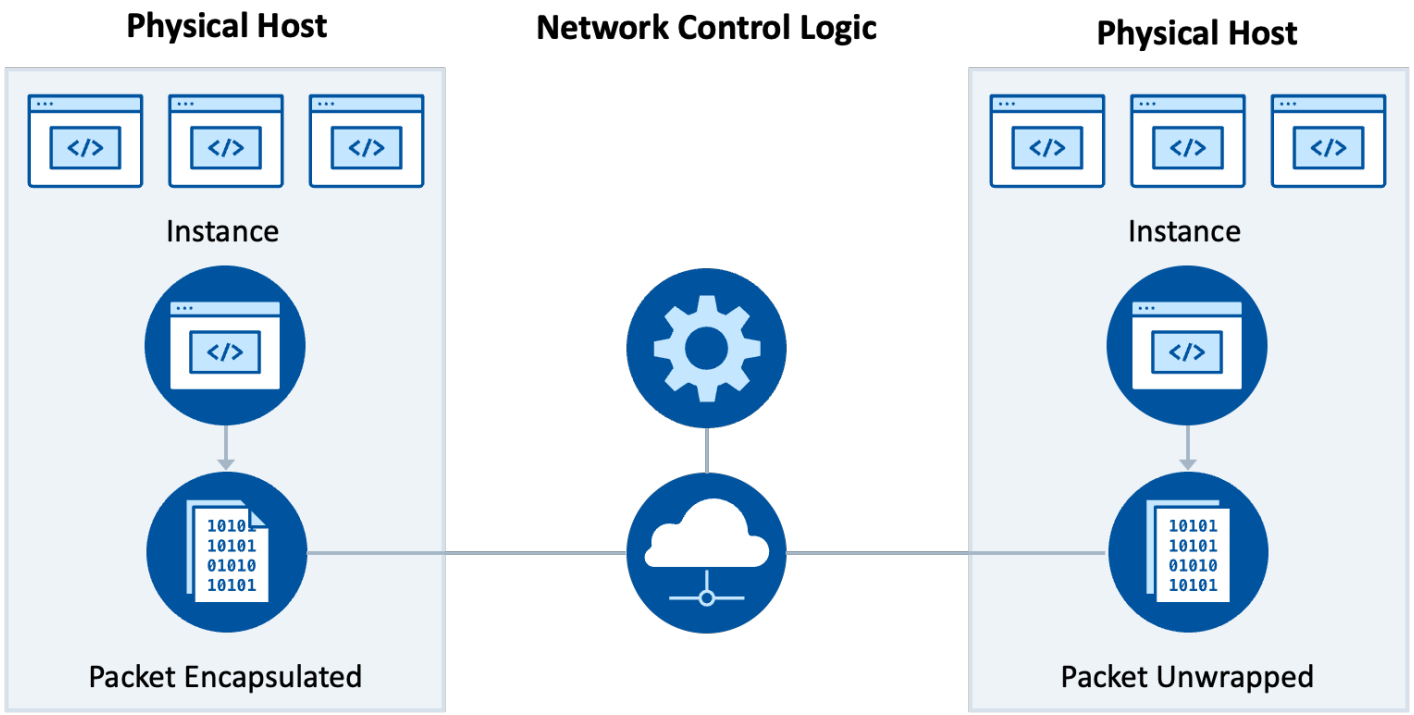
Structural

Traditional security that will change based on the deployment environment

Many Voices.
One Community.

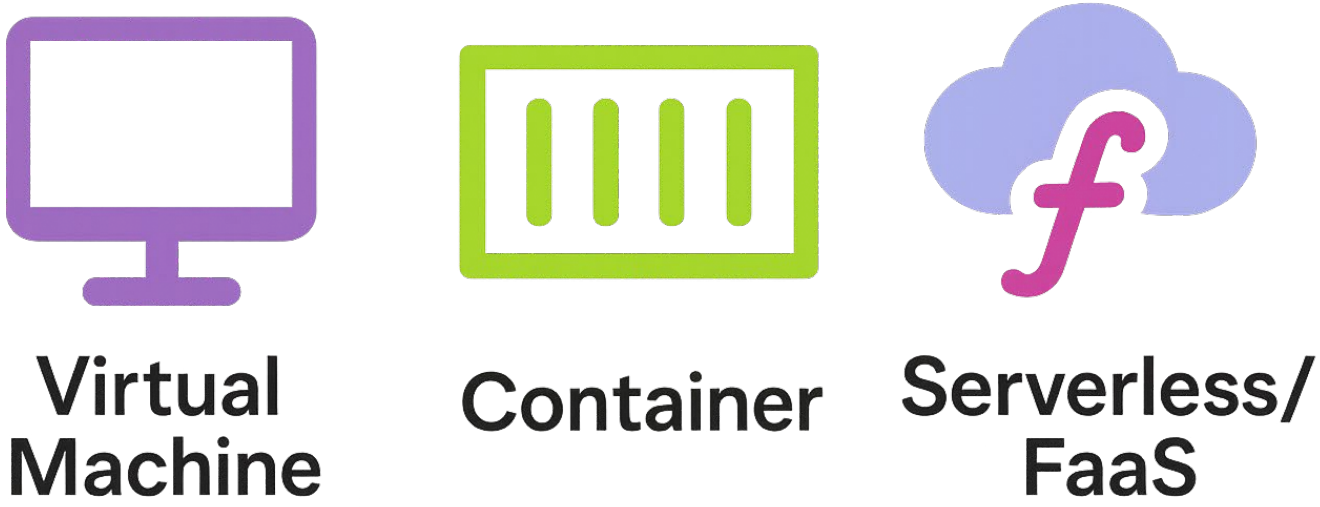
Network

- Software Defined Networks make *packet switched networks behave like circuit switched networks*
- Prefer cloud native over virtual appliance
- Use the *Minimum Viable Network* concept



Rules, rather than configurations, define network security

Workload



- Focus on images and pipelines
  - Ephemeral workloads deployed via CI/CD are more secure\
  - Software composition analysis is your best friend
- “Cattle vs. Pets”

Data

What's Different

- Everything potentially public with an API call
- More data
- Access control complexity
- *No inherent data perimeter*

What to Do

- Use org controls like Block Public Access
- CSPM to detect public
- IAM (best effort)
- Start on the data perimeter path

Application

- Use Platform as a Service to reduce the security management surface
  - And the security attack surface

- Infrastructure as Code in CI/CD Pipelines improve security
- Unless your pipeline is compromised
  - Focus on pipeline security
  - Embed security testing into pipelines
    - IaC scanning
    - SCA
    - SAST

Apply: Structural

- Use network architectures for network security
  - Segregation and isolation are the default (mostly)
  - Some capabilities are built into the fabric (security groups)
  - Minimize network security appliances, but most places still need some
- CI/CD pipelines from known good sources and ephemeral deployments are the core of workload security
- Focus on the data perimeter and locking down sharing/public
- PaaS is your friend and reduces attack surface

RSAC | 2025 Conference

Procedural

Core processes to improve maturity over time

Many Voices.
One Community.

Not for Beginners

Procedural Domains Categories to highlight the processes needed to protect your cloud (and keep it protected).						
Risk Assessment & Provider Management There are three aspects of risk assessment: 1. provider selection (choosing providers) 2. ongoing provider re-assessment and management 3. risk assessment of specific projects and programs.	Use existing risk assessment models and provider selection process.	Provider selection driven by business unit, but security assesses the provider and can trigger an escalation. Security inconsistently engaged in early project risk assessments (e.g. architecture risk).	Basic security standards for cloud providers of different service models (IaaS, PaaS, SaaS) in use. Initial provider registry in use, showing approvals by data classification/risk/compliance.	Security engaged with process for evaluating providers and deployments. Existing provider and deployment risk profiles re-assessed either annually, or after major change. Risk registry includes approvals at the service level.	Security-driven risk assessment for new projects and cloud migrations, with formal templating and remediation plans. Existing providers and projects are evaluated continuously for updated risk profiles.
Resilience Ensuring resiliant use of cloud that meets an organization's business requirements for availability and recovery.	No formal resiliency for cloud deployments.	Some basic data backup/lifecycles. Some use of autoscaling/ automation for workloads. Largely single provider/region deployments.	Moderate use of autoscaling/automation for workload resiliency, where possible. Initial use of multi-region resiliency. Some deployments use IaC for additional resiliency.	Most deployments provisioned with IaC. Some use of multi-region and multi-account resiliency. Deployments use assessable resiliency control specifications. Data-plane resilient to larger CSP failures.	All production deployments provisioned with IaC. IaC repositories implement resiliency. Automated failovers and redeployments in use. Chaos engineering in place.
Compliance & Audit Meeting regulatory compliance requirements and mandates.	No reporting or compliance actions taken for cloud-specific resources.	No cloud-specific standards. Ad-hoc assessment and remediation of deficiencies on cloud-based resources.	Cloud provider and service (SaaS or PaaS) approved list. Scheduled assessments of cloud providers. Manual reporting of cloud controls versus standards.	Continuous assessment of in-scope resources using automated guardrails, manual remediation of deficiencies. Reporting is partially automated.	Continuous assessment and automatic remediation of deficiencies using cloud automation. Reporting fully automated across all applicable standards with dashboarding.
Incident Response Cloud-specific incident response processes, including compromise of the cloud console/management plane.	No cloud-specific response, uses existing IR playbooks (if they exist).	Manual IR response to cloud events. Inconsistent data collection and escalation.	Consistent manual response with rudimentary tooling.	Trained responders using cloud-specific tooling and refined processes. Some platform-based automation (quarantine asset, take snapshot, etc.). Cloud native detection engineering.	Fully automated and orchestrated IR workflow backed by a cloud IR team and response platform. Testing using a cloud-focused Red Team and incident simulation.

- These are important, but come after the fundamentals
- The exception is Incident Response: consider outsourcing if you don't have cloud subject matter expertise internally
  - Incidents are already happening

The Final Apply

- Cloud is fundamentally different than traditional infrastructure, even when it looks the same
  - Learn to see what's different and your skills will catch up
- Focus on identity management first, especially static reds
  - And second
  - And third
  - Like, just do this for a year or two
- Don't expose things to the Internet

The Final Apply

- Focus your CSPM on finding public exposures and critical misconfigurations
- Get the authority to enforce baseline standards and fix things fast
  - A cloud misconfiguration is immediately exploitable, it isn't a vulnerability to patch in 90 days
- Hire SMEs for each cloud provider you use
  - No one is a real expert on more than one

More Help and Information

- The CSA/IANS/Securosis CSMM 2.0 (free without registration)
  - https://www.iansresearch.com/resources/cloud-security-maturity-model

- Cloud Security Alliance
  - Guidance: https://cloudsecurityalliance.org/research/guidance
  - CCM: https://cloudsecurityalliance.org/research/cloud-controls-matrix

- Cloud Security Lab a Week (CloudSLAW)
  - Free weekly hands-on security labs
  - https://slaw.securosis.com

RSAC 2025 Conference

Many Voices.
One Community.

Thank You

Rich Mogull

@rmogull (BSKY/Mastadon)

rmogull@securosis.com

slaw.securosis.com